From Cyber Security Risk Management to Operational Risk Management

Wim Mees
Royal Military Academy, Department CISS
Renaissancelaan 30, 1000 Brussel, Belgium
wim.mees@rma.ac.be

1.0 INTRODUCTION

Cybersecurity is inherently difficult. Protocols are insecure, software is vulnerable, network and system configurations change frequently, and end-users contribute more often to the problem than to the solution.

Since resources are limited, choices have to be made on where to invest resources to protect the information infrastructure. These choices are driven by a risk management approach. Traditional risk management approaches focus on known threat sources exploiting individual vulnerabilities and on security controls that provide point solutions to protect against them.

It is important to consider all possible threats, also those for which the current opponent does not (yet) have the necessary capabilities to exploit them. In a military environment it is part of the normal decision support process to continuously gather intelligence about the opponent(s) and use this information to develop and compare possible courses of action. The same approach must be adopted to address cyber-threats.

It is furthermore not the responsibility of a "cyber-decision maker" to decide about the way cyber-threats or cyber-opportunities are to be managed. Unity of command requires that the joint task force commander makes the decision, based on an overall risk assessment that covers all aspects of the operation.

Finally, we take a look at the *"Afghanistan Mission Network"* (AMN) to illustrate these different aspects of operational risk management.

2.0 THREAT MODELLING

After years of research and development in the area of network and system security, it is still not possible to design and implement secure systems or to evaluate the security of a given system in a scientifically meaningful way. One of the reasons why in civil or mechanical engineering there are well-defined processes for designing, building, and certifying for instance bridges and aircraft, is the fact that the forces they have to resist are due to natural and accidental causes, whereas in cyberspace

most of the "forces" to be addressed are driven by deliberate human intent and therefore much more difficult to predict and quantify. In order represent the forces working against the security of an information system, a *"threat model"* is needed.

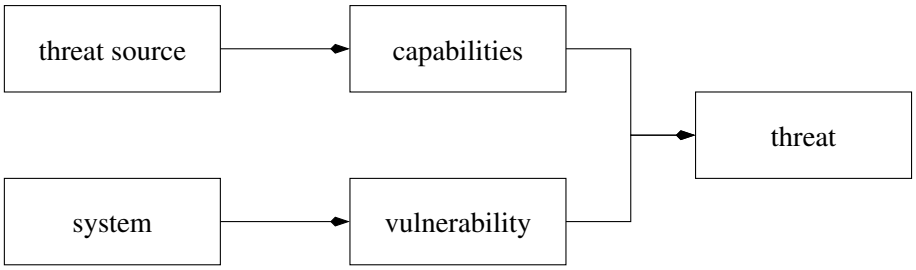

Figure 1: classic threat

Figure 1 show the threat assessment approach as it is nowadays performed in most organizations for the purpose of cybersecurity risk management [6]. The system for which the threats are to be assessed is scoped and modelled, and the known vulnerabilities for its assets are listed. In parallel the possible threat sources are identified, as well as their capabilities. When a threat-source is considered to have the necessary capabilities and motivation to exploit a given vulnerability, this is considered a threat that needs to be addressed. If there is no threat-source that has the capabilities or motivation to exploit the vulnerability, the approach considers that there is no threat and the vulnerability is no longer considered in the context of the risk management process.

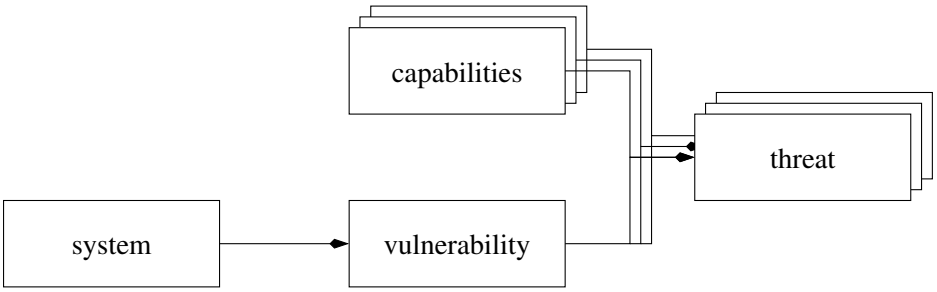

Figure 2: actionable threat

The *"actionable threat"* approach [4] however does not start from a given threat source and its capabilities. It rather considers different possible levels of capabilities that - in combination with a given vulnerability - result in different levels of threats, as is illustrated in figure 2. This makes it possible to identify a number of design options, with the corresponding security controls to be put in place to reduce the residual risk to a certain level.

Military information systems have long life-cycles and can over time be used in conflicts against a wide range of opponents. It is therefore important to consider all possible threats when designing systems and security controls, and not just those matching a (potentially long) list of threat sources which are considered to have sufficient motivation and skills in the context of a given operation.

It is thus important to consider an as exhaustive as possible list of possible threats with the capabilities that would be needed to instantiate the threat, and this independently of the currently known threat sources. The resulting set of potential threats is not opponent or military operation specific therefore highly reusable.

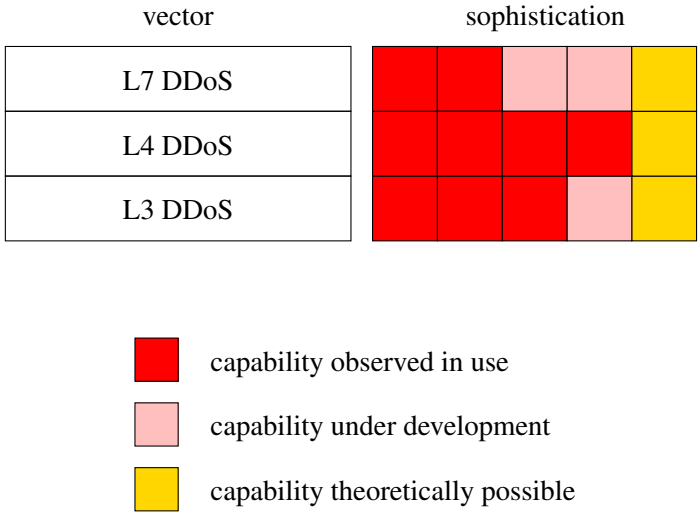

Figure 3: threat capabilities without controls

A capability consists of a vector and a sophistication level. An example with five sophistication levels is shown in figure 3 for three sample vectors. In this example we consider that readily available tools that implement the basic attack functionalities have been observed for the three vectors up to certain levels of sophistication. Other levels of sophistication are known to be under development, such as the massive use of *"Internet of Things"* (IoT) devices for launching DDoS attacks. The highest levels of sophistication may for instance require specific cryptographic attacks against hashing algorithms, and although theoretically possible they have not yet been observed in the wild.

The next step consists in mapping the already implemented controls on the capabilities, as is shown in figure 4. This results in an identification of the remaining capabilities that could result in a threat if there is a threat source that has these capabilities and the necessary motivation to apply them.

3.0 ADVERSARIAL BEHAVIOURAL MODELLING

Based on the threat analysis from the previous section, a number of capabilities were identified that could lead to unacceptable risks if an adversary were to apply them. The challenge is now to apply the limited cyber-security resources that are available in the best possible way.

This requires us to model the behaviour of the opponent in the context of the military operation, and how it will evolve in the near future. Predicting an opponent's behaviour is something that is systematically done in the context of an *"operational planning process"* (OPP), an example of which

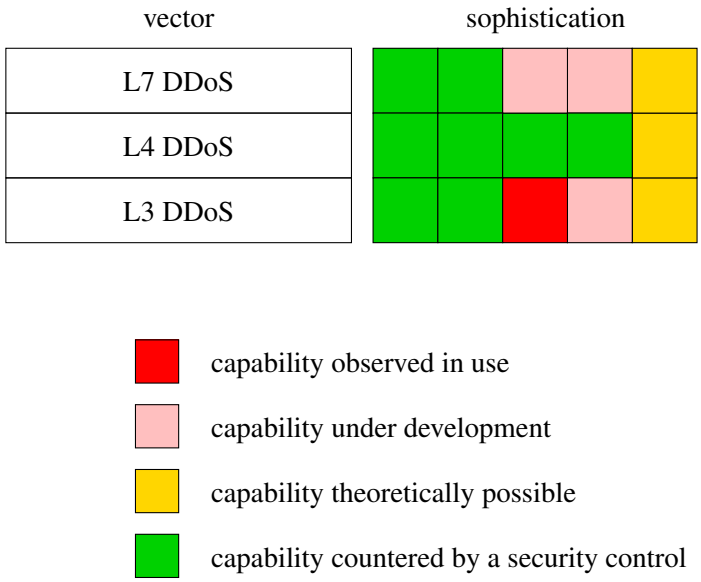

Figure 4: threat capabilities with controls

is shown in figure 5. Once the mission has been analyzed and the commander has given his planning guidance, the *"concept development"* phase starts during which the staff officers identify and develop possible *"courses of action"* (CoA) that have to be complete, feasible, consistent with doctrine, and in compliance with the commander's guidance. The CoA are then briefed to the commander who selects one of them. His staff will then produce the *"concept of operations"* (CONOPS), including a *"statement of requirements"* (SOR).

CoA development consists of war-gaming, risk assessment, and the comparison of the war-gaming results for the different CoA. Currently there are no examples that explain how to perform the cyber-side of CoA development. The regular CoA development is based on a process called the *" intelligence preparation of the battlefield"* (IPB), that combines the battlefield environment with what is known about the enemy's doctrine in order to determine how the enemy will most probably try to complete his mission.

In order to perform a cyber-IPB, we need to be able to model adversary behaviour and defender-attacker interactions in cyber-space. Researchers often assume a homogeneous adversary population, and extract a single adversary behaviour model [5]. Recent work by Abbasi et al. [1] has however shown that the inherent heterogeneity in adversary behaviour can be better captured by clustering adversaries into distinct groups with different model parameters per group, and that this results in more accurate predictions of future behaviour.

Figure 6 shows the result of the cyber-IPB modelling of adversary capabilities. Two groups of opponents have been found, with capability sophistication levels shown as E_1 and E_2. Additional intelligence could for instance reveal that E_1 consists of highly motivated insurgents that are actively involved in the conflict, whereas E_2 is a hostile nation that sympathizes with the insurgents but will most likely not undertake any action yet at this stage of the conflict.

This brings us to the problem of *"attack attribution"*, a term which can have different meanings

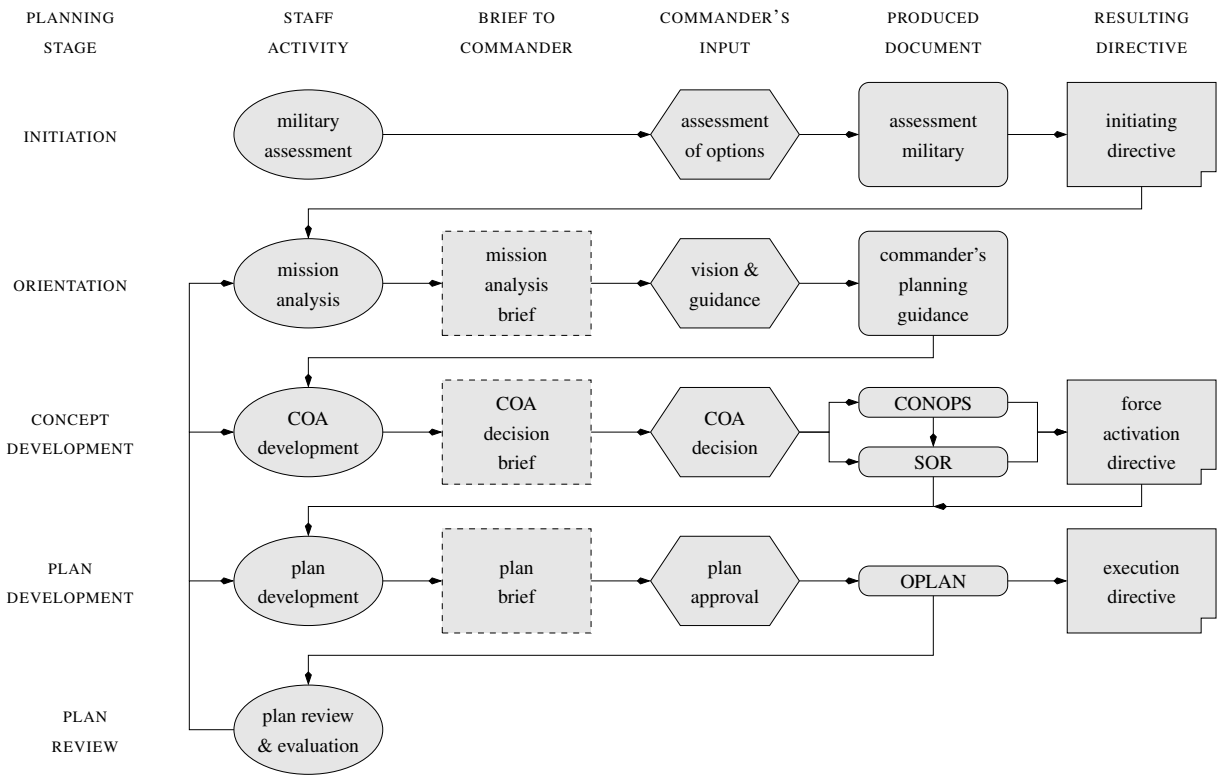

Figure 5: operational planning process

to different people. A basic level of attribution consists of grouping multiple hostile activities in order to identify an opponent or an opponent's campaign. A complete attribution however also involves identifying the people, organisation or nation that is behind an attack.

Some people argue that absolute attribution allows a defender to predict more easily what the ultimate goal is that the attacker is after. The problem is that this often leads to cognitive bias [9], and as a result the analyst will start looking at the data differently in the hypothesis that a certain opponent is behind the events he observes, which may in turn lead to incorrect conclusions.

4.0 SITUATION AWARENESS

Two important models for representing decision making in a military context are Boyd's *"observe - orient - decide - act"* (OODA) loop [2] and Endsley's decision making model with three levels of situation awareness [3]. Level 1 SA, called *"perception"*, is the direct equivalent of the OODA observe process, while level 2 SA, called *"understanding"*, corresponds with the OODA orient process. Level 3 SA, called *"projection"*, however has no direct equivalent in the OODA loop. It can be considered as a combination of the higher level knowledge produced by the orient process, that makes it possible to project into the future, and the COA development that is part of Boyd's decide process.

Figure 7 shows an attempt at uniting Boyd's OODA loop model and Endsley's decision making model. It incorporates a separate planning stage, as is suggested by a number of authors [7]. On the

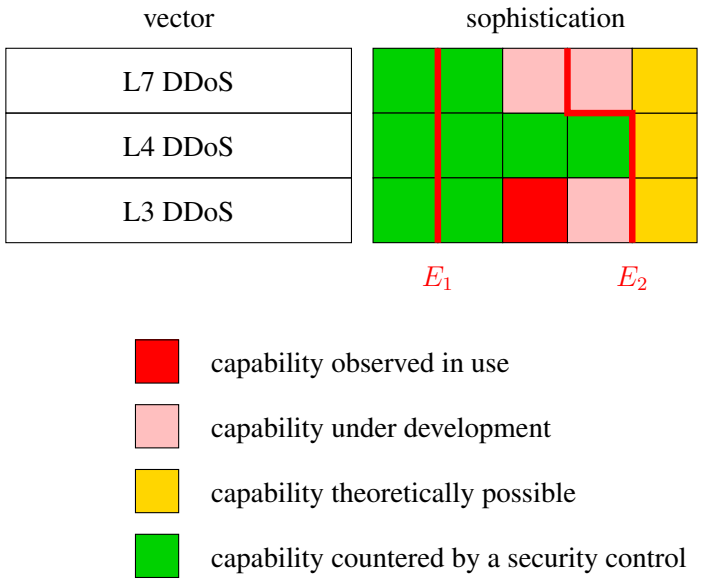

Figure 6: adversary behavior modelling

left a map of the *"situtation awareness"* (SA) is drawn.

We have followed Endsley's approach of having the SA cover the entire range from the low-level raw data acquisition processes up to the synthesis of a deeper understanding of also the cyber aspects of the operation. We do however still distinguish within that SA the elements that make up the *"operational picture"* (OP) from the higher levels of knowledge and understanding, since it will typically be that information that is managed and exchanged by the already existing *"network operations centers"* NOCs or *"cybersecurity operations centers"* CSOCs, as well by the existing operational Command & Control Information Systems (CCIS) for the kinetic aspects.

Three different information flows are indicated by numbered arrows in figure 7:

(1) Information enters the SA at different levels of the cognitive hierarchy. At the lowest levels it is for instance raw sensor data, like netflow data or firewall logs, a level higher it can be processed information that is exchanged between friendly forces in the context of a *"common operational picture"* (COP), while at the highest levels it can consist of operational or strategic intelligence reports.

(2) A lot of information enters the SA, much of which is volatile and only relevant for a short period of time and can thereafter be "forgotten". The part that is relevant for a longer period of time migrates from the "volatile" to the "persistent" part of the SA.

(3) The ultimate goal of developing SA is to support the decision making process by making it possible in the planning stage to identify and evaluate COAs. It is therefore important to process the lower levels into higher level SA, be it through the "manual labour" of human analysts or through automated processing, using signal processing, pattern recognition, correlation and aggregation, information fusion, artificial intelligence, security analytics, ...

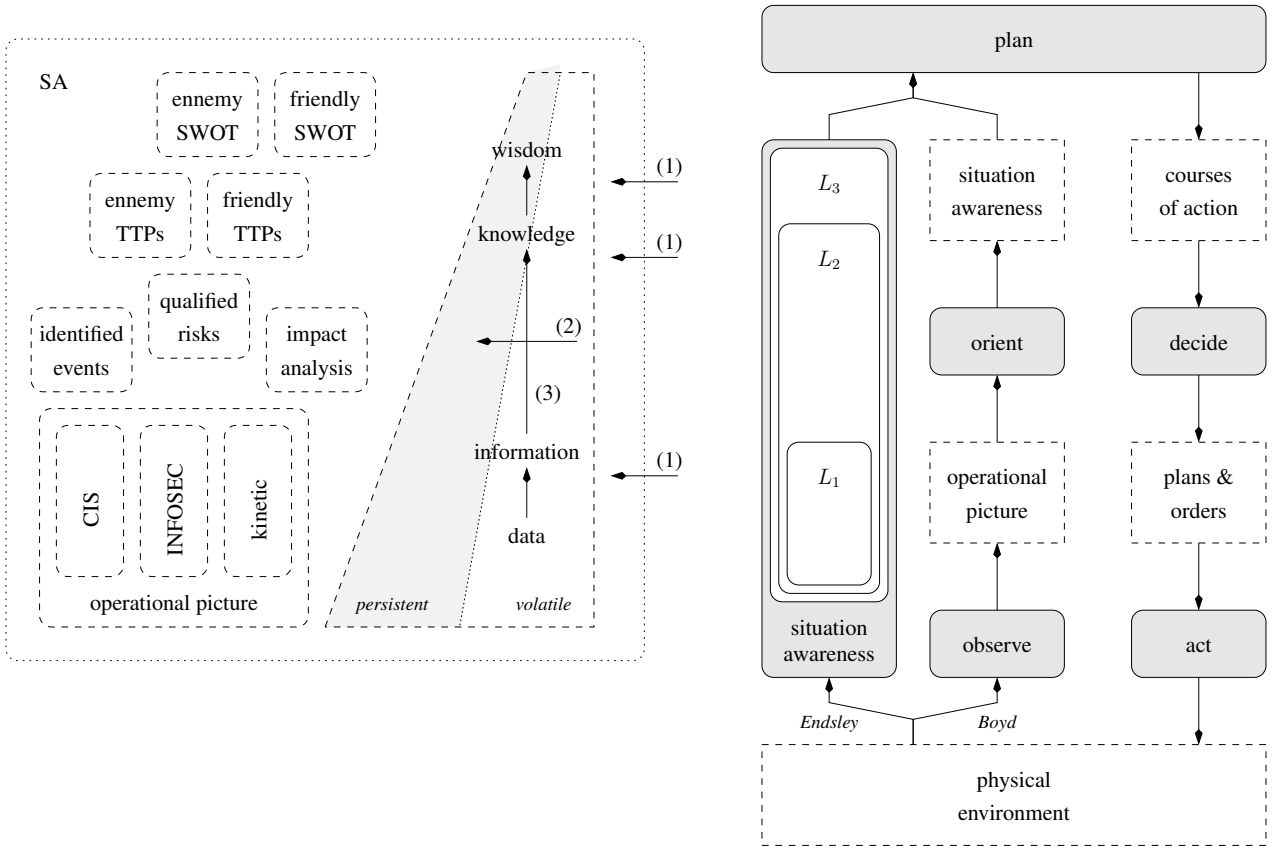

Figure 7: situation awareness

We have deliberately not drawn a separate *"cyberdefense situation awareness"* in figure 7. Indeed, even though in practice at lower levels different systems may be used, resulting in an aggregate COP, it is important to have at the level of the decision support staff a single SA that is used for COA development and comparison.

Unity of command is one of the twelve principles of joint operations [14]. It requires that all forces operate under a single commander who directs all forces in pursuit of a common purpose. There cannot be a separate cyber decision making process that performs cyber risk management based on a cyber situation awareness. It is the operational commander who decides based on a advise from specialists in the different areas.

This means that the operational commander must have at least a high-level view and understanding of the cyber-situation. In [8] a multi-aspect 3D visualization is proposed that could be used to communicate to a military commander the situation of his assets in cyberspace, their importance to the mission, the threats they are exposed to, and finally the adequacy of the security controls in place to protect it.

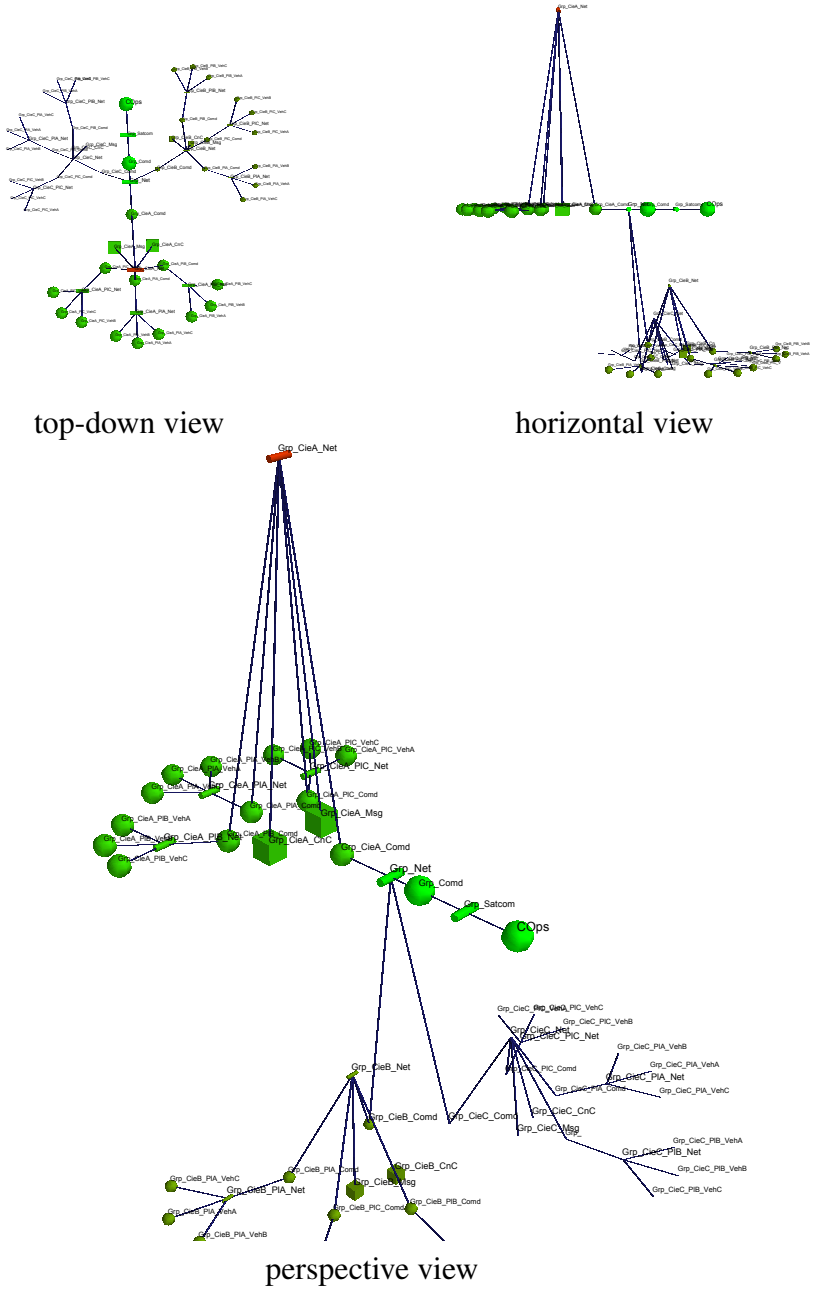

Figure 8: visualization

An example of this visualization is shown in figure 8. The principal elements of information are encoded in the following ways:

- *shape:* different classes of assets are represented by different shapes that are easily distinguishable and recognizable,
- *size:* when the size of a symbol is bigger, this means that the represented asset is more important to the mission,

- *color:* when the color of a symbol is closer to red a lot of interest in this asset is observed on behalf of the opponent, whereas when the color is closer to green, there is less or no hostile activity observed against the asset,
- *height:* when symbols are "tied down" close to the ground this means their security is considered to be well controlled, whereas when they are floating up high in the air they are more at risk of "breaking off and flying away in a storm",
- *motion:* motion represents change, therefore when one or more characteristics of an asset are changing, the symbol representing the asset will be shaking, with an amplitude that reflects the intensity of the change.

The 3D view is based on a conceptual "spring-model", called "Mission - Attacker - Controls" (MAC) triangle, per asset, which considers various planning factors that the commander and his staff should take into account. The components of the forces that are represented by the springs in the MAC triangle are derived from low-level security metrics that are in turn based on low-level data and measurements. This low-level information is evaluated using fuzzy domain knowledge and approximate reasoning and finally aggregated into a single value that quantifies the strength of each force component.

5.0 CASE STUDY

As a result of the Bonn Conference in December 2001 the *"International Security Assistance Force"* (ISAF) was created. It's primary objective was to assist the Afghan government in providing effective security across the country, as mandated by the United Nations. In August 2003 NATO took the lead of ISAF, ending the national six-month rotations of command. As a result NATO became responsible for providing a force commander with his headquarters on the ground in Afghanistan and had to set up a command and control infrastructure.

ISAF command and control rapidly faced the challenge of an information overload. Information was abundantly available from military units in the field, local and national authorities, regional and international media, fact-finding teams, governmental and non-governmental organizations, etc. Unfortunately the information was often ambiguous or incomplete, sometimes even contradictory or inconsistent. The long-standing security restrictions and the incompatibilities between the different information systems resulted in essential mission information that remained stove-piped in separate national and international systems and was not properly exchanged [13].

The lack of a fluent exchange of information between the participants in the operation soon caused important problems, especially given the *"counter-insurgency"* (COIN) nature of the operations that strongly depends on the availability of intelligence. In 2006 an effort was undertaken to make the exchange of email messages possible between the US mission network at that time, which was the "Combined Enterprise Regional Information Exchange System" (CENTRIXS) "Global Counter Task Force" (GCTF), and the ISAF SECRET network used for conducting the NATO operations. This resulted in a complex architecture with various guards, firewalls and intrusion detection systems that made the exchange of email possible. It was however so difficult to use and to administer that at some point it failed for 35 days without this incident even being reported. Another effort to establish

the exchange of information between the NATO network and national networks was lead by the UK and made use of their OVERTASK network. Operating on the same network required however a centralised configuration control and this created problems for the individual nations trying to operate their nationally-owned solutions.

In 2008 NATO funded an effort to provide voice, chat and web access over the UK OVERTASK network, but the US was still using its own national solution, at that time the *"Secret Internet Protocol Router Network"* (SIPRnet), and had no real solution to communicate with the coalition partners at a secret level. General Stanley McChrystal, at the time commander of the ISAF and US Forces Afghanistan, realized that a real-time common operational picture and shared situation awareness were essential, and required in 2009 that a single *"Afghanistan Mission Network"* (AMN) be created that would allow all coalition partners to share classified information efficiently, as was proposed at the USCENTCOM Network Operations (NETOPS) conference held in Qatar in 2008 [13]:

> "If you need to do your mission with unstructured data, running it through guards will break your sharing AND doesn't even make for effective risk mitigation. Don't use guards if you want robust sharing with NATO. [Instead] turn GCTF in Afghanistan into CENTRIXS-ISAF so the CENTRIXS-to-NATO ISAF boundary is no longer a cross-domain boundary. Make CENTRIXS-ISAF the primary mission network and try to move U.S. users onto that network for the Afghanistan mission."

In April 2010 NATO's resource committees formally approved the way ahead for the AMN project and initial operating capability was declared in July 2010, meaning that the AMN was available to at least 50% of all ISAF forces. AMN provided email, web browsing, blue force tracking, chat, VoIP voice communications and video teleconferencing. It interconnected the US CENTRIXS (Combined Enterprise Regional Information Exchange System), which is the theater version of SIPRNet, with NATO's ISAF Secret network, to which the other ISAF nations in turn connected. Over time 165 applications were moved to the shared network, 55 of which are considered critical to the mission [10].

Before the creation of the AMN the national commanders had to gather at a central location to discuss plans and exchange information, often using removable media to manually transfer information from one system to another, introducing unacceptable delays. The AMN radically changed the way the ISAF nations share mission information, situational awareness and commander's intent across the battlefield. As the nations use different command and control software to visualize data, the data is published on a common server where the users subscribe to it and import it into their national systems, such as "Command Post of the Future" for the US, or JADOCS for the UK. Another complication is the fact that the typical blue versus red opposition that lies at the basis of many command & control data models is no longer the main concern for the commanders at different levels. Indeed, the green Afghan government and security forces symbols as well as the white symbols that represent local population centres are just as important. Often the objective of the commander consists in separating red from white, and in inserting green elements in between. In order to facilitate the exchange of non-conventional types of information, for instance obtained from human intelligence, that do not necessarily fit in the existing data models, a Wiki functionality was integrated in the AMN [12].

The AMN is a good example of the paradigm shift from focussing on the mitigation of risks by implementing strict controls in order to restrict access to information on a need-to-know basis to

exploiting the opportunities that information technology offers in order to satisfy the need-to-share requirement that is essential in current-day agile coalition-based warfare. Unfortunately, relaxing certain security constraints in order to allow for a very agile response to evolving user requirements when this results in an important operational benefit, can result in an increased number of information security incidents. The AMN is a flat and open network, allowing users to obtain information without firewalls, logins, passwords or certificates. As a result everybody shares the same basic risk that every other user is a vulnerability. This resulted in the spreading of the Conficker virus, known since 2008, in the AMN network in 2011. Because of the risk mitigation controls in place, the virus was however picked up rather quickly and after about five hours normal operation was restored [11].

6.0 CONCLUSIONS

In this paper we have presented a number of aspects that can influence the decisions made while managing cyber risks in an operational context.

To start with, we have to look at all possible threats, considering different capability levels that potential attackers might have, when designing systems and security controls.

In the context of a given military operation we then have to integrate cyber-space specific considerations into the joint operational planning process. This involves war-gaming in order to develop possible courses of action and therefore we need adversarial behavioural modelling.

Finally it is up to commander to make the decisions, so he needs to have joint situation awareness, and this includes cyberspace. Therefore visualizations are needed that allow him to grasp the impact of the situation in cyber-space on his decisions and vice versa.

REFERENCES

[1] Yasaman D Abbasi, Noam Ben-Asher, Cleotilde Gonzalez, Debarun Kar, Don Morrison, Nicole Sintov, and Milind Tambe. Know your adversary: Insights for a better adversarial behavioral model.

[2] John R Boyd. Organic design for command and control. *A discourse on winning and losing*, 1987.

[3] Mica R. Endsley. Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1):32–64, 1995. doi: 10.1518/001872095779049543.

[4] Rich Goyette, Yan Robichaud, and François Marinier. A research agenda for security engineering. *Technology Innovation Management Review*, 3(8):41, 2013.

[5] Debarun Kar, Fei Fang, Francesco Delle Fave, Nicole Sintov, and Milind Tambe. A game of thrones: when human behavior models compete in repeated stackelberg security games. In *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*, pages 1381–1390. International Foundation for Autonomous Agents and Multiagent Systems, 2015.

[6] Wim Mees. Risk management in coalition networks. In *Third international symposium on information assurance and security*, pages 329–336. IEEE, 2007.

[7] Wim Mees and Thibault Debatty. An attempt at defining cyberdefense situation awareness in the context of command & control. In *Military Communications and Information Systems (ICMCIS), 2015 International Conference on*, pages 1–9. IEEE, 2015.

[8] Wim Mees, Salvador Llopis, and Thibault Debatty. Achieving cyber situation awareness through a multi-aspect 3d operational picture. In *IST-148 Symposium on Cyber Defence Situation Awareness*. NATO STO, 2016.

[9] Marco Riccardi. *APPLYING INTELLIGENCE ANALYSIS WHILE ATTRIBUTING CYBER ATTACKS*. PhD thesis, Utica College, 2016.

[10] Barry Rosenberg. Battlefield network connects allied forces in afghanistan. *Defense Systems*, September 2010.

[11] George I. Seffers. Conficker worms its way into afghan mission network. *AFCEA Signal*, April 2011.

[12] George I. Seffers. France joins afghan mission network. *AFCEA Signal*, May 2011.

[13] Chad C. Serena, Isaac R. Porche III, Joel B. Predd, Jan Osburg, and Bradley Lossing. Lessons learned from the afghan mission network - developing a coalition contingency network. Technical Report ISBN 978-0-8330-8511-5, RAND Corporation, 2014.

[14] Joint Staff. Joint publication 3-0: Joint operations, 2006.